Mobile Payment System

Cryptography

PayMobile 2.0
February-March 2010

История изменений

Дата	Автор	Описание
22.02.2010	Тулепов Е.А.	Создан

Оглавление

1 Сокращения

1.1 Общие

ВДО	Select For Update DML.
ЗИД	Защитный Идентификатор Договора.
ЗО	Запрос на Обслуживание.
ИАП	Идентификатор Алгоритма Подписи.
ИКМК	Индекс КМК.
ИП	Идентификатор Процессора.
КЗО	Контроллер Запросов на Обслуживание.
КМК	Корневой МК.
МК	Мастер Ключ.
СЖ	Системный Журнал.
СМПП	SMPP.
СМС	SMS.
СП	Счетчик Подписей.
СЧ	Случайное Число.
ХТТПС	HTTPS соединение.
ШС	Шифрованное TLS/SSL Соединение.

1.2 Специфические

ДЗ	Дата Заявления.
КК	Клиентский Ключ.
ПК	Подписывающий Ключ.

2 МК под паролем

2.1 Диверсификация клиентского ключа

$KK = U_1 \oplus U_2 \oplus \ldots \oplus U_N$,

где $U_1 = PRF(Пароль, Соль \,||\, L)$, $U_2 = PRF(Пароль, U_1)$, …, $U_N = PRF(Пароль, U_{N-1})$

PRF	Длина Соли, байт	N	L
HMAC-SHA-1	20	1024	$00A0_{16}$
HMAC-SHA-256	32	1024	0100_{16}

2.2 Получение МК

$МК_{Ч} = КК \oplus МК_{Х}$,

где $МК_{Ч}$ — чистый МК;

$МК_{Х}$ — МК, хранящийся в мидлете.

2.3 Требования к паролю

1. Набор символов.
2. Длина.
3. Не должен быть равен № телефона, заявки.
4. Минимальное количество чисел, букв и специальных символов, если они есть в наборе.
5. Максимальное количество одинаковых символов.

При выборе критериев должен учитываться компромисс между сложностью и не вынуждением пользователей прибегать к упрощению паролей, записыванию паролей и т.д.

3 Диверсификация ключей

$K_O = PRF (K_I, Label || Context || L)$

3.1 МК из КМК

PRF	Длина $K_{I,O}$, байт	Label	L
HMAC-SHA-1	20	MKHMS00	$00A0_{16}$
HMAC-SHA-256	32	MKHMS01	0100_{16}

Значения поля Label должны быть представлены в форме DataOutput.WriteUTF до конкатенации.

Context	Формат	Длина, байт	Примечания
№ телефона	X...X	8	
ЗИД	X...X	8	
ДЗ	ССМИЧЧ24ДДММГГ	12	
ИКМК	XX	1	
ИП	XXXX	2	

Значения поля Формат, кроме ДЗ, должны быть представлены в форме целого до конкатенации.

3.2 ПК из МК

PRF	Длина $K_{I,O}$, байт	Label	L
HMAC-SHA-1	20	SKHMS00	$00A0_{16}$
HMAC-SHA-256	32	SKHMS01	0100_{16}

Значения поля Label должны быть представлены в форме DataOutput.WriteUTF до конкатенации.

Context	Формат	Длина, байт	Примечания
СЧ	X...X	20-32	
СП	XXXX	2	
№ телефона	X...X	8	
ЗИД	X...X	8	
ИКМК	XX	1	
ИАП	XX	1	
ИП	XXXX	2	

Значения поля Формат должны быть представлены в форме целого до конкатенации.

4 Подписывание

4.1 Алгоритмы

Алгоритм	ИАП	Длина ключа, байт
HMAC-SHA-1	00_{16}	20
HMAC-SHA-256	01_{16}	32

4.2 Данные

Поля\Операции	Перевод	Выписка	Остаток	Обновление счетов
СЧ	X	X	X	X
СП	X	X	X	X
Сумма	X			
Код валюты	X			
КНП	X			
Описание	X			
Имя счета отправителя	X	X	X	
Имя счета получателя	X			
Тип выписки		X		
Тип	X	X	X	X

Поля\Операции	Перевод	Выписка	Остаток	Обновление счетов
№ телефона	X	X	X	X
ЗИД	X	X	X	X
ИКМК	X	X	X	X
ИАП	X	X	X	X
ИП	X	X	X	X

Поля должны конкатенироваться в представленной последовательности.

5 Криптопериоды

Рекомендуемые криптопериоды по NIST SP 800-57 Part 1 для:

1. КМК, МК — около 1 года;
2. ПК — <= 2 лет.